

Rec'd PTO

03 OCT 2003



10/57011
PCT / IB 0 3 / 0 4 4 8 4

08 OCT 2003

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

REC'D 17 OCT 2003

WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

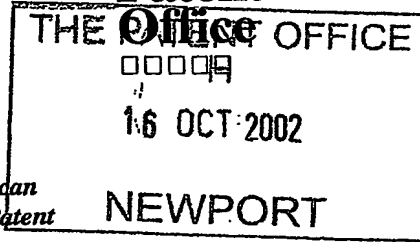
Signed

Dated 15 July 2003

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

BEST AVAILABLE COPY

An Executive Agency of the Department of Trade and Industry



170CT02 E756199-1 D02879
P01/7700 0.00-0224041.4

The Patent Office
Cardiff Road
Newport NP10 8QQ

request for grant of a patent
see notes on the back of this form. You can
so get an explanatory leaflet from the Patent
Office to help you fill in this form)

Your reference

PHGB020176

Patent application number
(The Patent Office will fill in this part)

0224041.4

16 OCT 2002

Full name, address and postcode of the or of
each applicant (underline all surnames)

KONINKLIJKE PHILIPS ELECTRONICS N.V.
GROENEWOUDSEWEG 1
5621 BA EINDHOVEN
THE NETHERLANDS

Patents ADP Number (if you know it)

7419274001

If the applicant is a corporate body, give the
country/state of its incorporation

THE NETHERLANDS

Title of the invention

VALIDATING A USER

Name of your agent (if you have one)
"Address for service" in the United Kingdom
to which all correspondence should be sent
(including the postcode)

Andrew G. WHITE
Philips Intellectual Property and Standards
Cross Oak Lane
Redhill
Surrey RH1 5HA

7133473003

Patents ADP number (if you know it)

If you are declaring priority from one or more
earlier patent applications, give the country
and the date of filing of the or of each of these
earlier applications and (if you know it) the or
each application number

Country

Priority Application number
(if you know it)

Date of filing
(day/month/year)

If this application is divided or otherwise
derived from an earlier UK application, give
the number and the filing date of the earlier
application

Number of earlier application

Date of filing
(day/month/year)

Is a statement of inventorship and of right to
grant of a patent required in support of this
request? (Answer "Yes" if:

YES

- a) any applicant named in part 3 is not an inventor, or
 - b) there is an inventor who is not named as an applicant, or
 - c) any named applicant is a corporate body.
- See note (d))

1. Enter the number of sheets for any of the following items you are filing with this form.
Do not count copies of the same document.

Continuation sheets of this form

Description
Claims(s)
Abstract
Drawings

7 /
2 /
1 /
4

only June

0. If you are also filing any of the following, state how many against each item:

Priority Documents

Translations of priority documents

Statement of inventorship and right to grant of a patent (*Patents Form 7/77*)

Request for preliminary examination and search (*Patents Form 9/77*)

Request for substantive examination (*Patents Form 10/77*)

Any other documents
(*Please specify*)

I/We request the grant of a patent on the basis of this application.

Signature

[Signature]

Date 15/10/2002

2. Name and daytime telephone number of person to contact in the United Kingdom

01293 815438

(A.G. White)

Warning.
After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.

Write your answers in capital letters using black ink or you may type them.

If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

If you have answered "Yes" Patents Form 7/77 will need to be filed.

Once you have filled in the form you must remember to sign and date it.

For details of the fee and ways to pay please contact the Patent Office.

DESCRIPTION**VALIDATING A USER**

5 This invention relates to a method of validating a user, and to a device and a system for implementing the method. This invention relates also to a software product, and to a computer readable medium.

10 When a designer determines how long a password or passnumber must be and what nature it must take in designing a system or device, a compromise needs to be made between the security conferred by the pass and the memorability of it. Short passes, such as the four-number passes commonly used with ATMs (automatic teller machines) do not confer a great deal of security (the number of possible combinations - including "0000" - is
15 just 10,000). Longer passes, on the other hand, especially numeric passes, are easy to forget. Passwords are generally considered as easier to remember than passnumbers of the same length. However, passwords are not easily usable with numeric input devices such as telephone keypads and television or video player remote controls.

20 Systems which involve strings of words in user validation are disclosed in JP 09-114785, JP 2001-053739 and WO 00/57370. Other user authentication systems are disclosed in US 6,035,406 and JP 07-336348.

25 It is an aim of the invention to provide a user validation system, device and method which achieves the security and inputability benefits found with numeric passes and the memorability benefits found with word-passed passes.

30 According to a first aspect of the invention, there is provided a method of validating a user, the method comprising associating a pass-sentence comprising a string of word blocks (Z_1, Z_2, \dots, Z_N) with the user, associating a passnumber comprising a string of numeric characters (Y_1, Y_2, \dots, Y_N) with the user, generating from the passnumber and the pass-sentence a table having columns in a vertical or horizontal direction and rows in the other direction, in

which each word block of the pass-sentence (Z_p) is located in a column dependent on the number of preceding word blocks ($P-1$) in the pass-sentence and in a row dependent on the corresponding character (Y_p) in the pass-sentence, displaying the table, receiving an input comprising a string of
5 numeric characters, comparing the input to the passnumber, and determining if the input is a valid input on the basis of the comparison.

The generating step may comprise recalling the table from a storage device. Preferably, though, the generating step comprises generating the table at random, allowing the passnumber to vary on each occasion of
10 requiring the passnumber. Preferably word blocks for use in generating the table are stored in a storage device. More preferably the number of word blocks stored in the storage device is approximately equal to the number of word block spaces in the table. This can allow the table to vary on each occasion whilst using the same word blocks, so that the pass-sentence cannot
15 be deduced by examining different tables and identifying word blocks common to the tables. Preferably, the table is filled with words such that each of the possible routes from one side to the opposite side produces a grammatically correct sentence. This may be achieved by filling the cells in each column with words of the same type, e.g. pronoun, adjective, past-participle, or with word
20 strings of the same type.

The invention also comprises a software product comprising computer executable instructions for carrying out the above method, and computer readable media having stored therein such a software product.

The invention also provides a device arranged for implementing the
25 above method, and a system arranged for implementing the method.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, of which:

Figure 1 is a flowchart illustrating a method according to one aspect of
30 the invention;

Figures 2 and 3 are schematic diagrams illustrating respective embodiments of devices according to one aspect of the invention.

Figure 4 is a schematic diagram of a system according to one aspect of the invention;

Figure 5 is a flowchart illustrating operation of the components of the Figure 4 system; and

5 Figure 6 is a schematic diagram of a second embodied system, according to one aspect of the invention.

A method of verifying a user is now described with reference to Figure 1. Referring to Figure 1, the method 10 begins at step 11, after which a pass-sentence is associated with the user at step 12. This step involves the reading
10 from an electronic memory a string of word blocks which in sequence form a sentence known to the user. In this example, the pass-sentence ($Z_1, Z_2 \dots Z_N$) comprises the following sequence (separate word blocks are included within brackets): (I) (walked) (to the) (zoo) (and) (saw) (a) (monkey). At step 13, a
15 pass number ($Y_1, Y_2 \dots Y_N$) is associated with the user. The passnumber comprises a string of numbers between 0 and 9, the length of the string (the number of numbers) being equal to the number N of word blocks in the pass-sentence (here $N=8$). In this example, the passnumber is 64310972. At step 14, a table is generated. The table has $N+1$ columns, and ten rows. The first
20 column is filled with digits 0 to 9 sequentially from top to bottom. The word blocks Z_1 to Z_8 are each included in the table at a position dictated by the value of the corresponding digit in the passnumber and the number of the word block in the pass-sentence. The relationship can be defined thus: Z_p is placed in column $P+1$ and in row Y_p . The other cells in the table are then filled
25 with suitable word blocks so that each column contains word blocks of the same type, for example nouns, articles, past participles etc. This allows a number of sentences equal to 10^N to be readable from left to right across the table. Most of these sentences will be nonsensical, but each will be grammatically correct. At step 15, the table is displayed. An example is
30 shown in table 1.

0	Fred	ran	through the	car	and	threw	ones	tree
1	They	went	up the	zoo	then	slapped	the	shoe
2	Ma	sailed	across the	theatre	and	melted	its	monk
3	Rick	thought	to the	hill	then	breathe d	their	bucket
4	She	walked	by the	box	but	froze	my	ticket
5	He	saw	around the	tourist	but	kicked	her	bike
6	I	talked	about the	bus	and	hung	mum's	duster
7	Pa	rode	against the	car	but	dribbled	a	mug
8	Rob	swam	under the	TV	then	dropped	his	trolley
9	Peter	flew	into the	mallet	and	saw	dad's	face

Table 1

A user knowing their pass-sentence and seeing the table then
 5 determines their passnumber. This is done by finding the row in the second
 column in which the first word block in their pass-sentence is found, and
 tracing that to the first column to find the corresponding digit. This continues
 for each subsequent column until the passnumber is found. This is then
 entered, using a keypad for example. Of course, the user may enter each digit
 10 as it is determined from the table, to avoid having to remember N digits before
 entering the passnumber. The method 10 remains at step 16 until a
 passnumber is entered. On receiving an input, it is compared at step 17 to the
 passnumber from step 13. If the comparison step 17 determines that the
 numbers are the same, then step 18 determines that the user is valid. In this
 15 connection, it will be appreciated that where plural rows in a column contain
 the same word block, any of the digits corresponding to the correct word block
 is acceptable. Viewed differently, it might be considered that there are plural
 valid passnumbers, one for each combination of word blocks which in
 sequence form the pass-sentence. If the input is not the same as the
 20 passnumber, an invalid user determination is made at step 18. The method 10
 ends at step 19.

Apparatus for implementing the method of Figure 1 is shown in Figure
 2. Referring to Figure 2, a mobile telephone is shown schematically at 20. It
 includes a CPU (central processing unit) 21, which is connected to each of a

memory 22, a display 23 and a numeric keypad 24. Audio message handling means (not shown) including transceiver, microphone and speaker or earpiece will also be provided. The CPU 21 is loaded with software from the memory 22 suitable for controlling the CPU to carry out the steps 12-14 of Figure 1.

5 Here, there is no 'user logon' step. At step 15, the table is displayed on the display 23, following which an input is entered by a user using the keypad 24. The CPU 21 then carries out steps 17 and 18 of the method 10. The pass-sentence is preferably stored in the memory 22, for recalling by the CPU 21 at step 12. Alternatively, the pass-sentence may be received as an SMS

10 message, for example.

Alternative apparatus is shown in Figure 3. Here, a television 30 is operated by a user through a remote control 31, which sends infra red signals dependent on keys pressed on a keypad 32 including numbers 0 to 9. These signals are received at an infra red receiver 33, which is connected to a CPU

15 34 along with a memory 35 and a display control 36. Operation is the same as with the Figure 2 embodiment, except that input is made by a user using the keypad 32 on the remote control 31.

A system implementing the Figure 1 method is shown in Figure 4. Referring to Figure 4, the system 40 comprises a server computer 41 and a

20 client computer 42. The server computer 41 includes a communications module 43 and a memory 44, each connected to a CPU 45.

At the other end of a secure link 46, a communications module 47 in the client 42 enables communication with the server 41. A CPU 48 is connected to the communications module 47, to a display 49 and to a keypad 50. The

25 server computer 41 may be a banking computer and the client 42 an ATM, for example. Operation will now be described with reference to Figure 5.

Referring to Figure 5, a first operation 51 is run on the server 41, and a second operation 52 is run on the client 42. User details are received at the client 42 at step 52a, for example from a magnetic account card (not shown).

30 The user details are sent at step 52b to the server 41, where they are received at step 51a. Meanwhile, the client 42 awaits input of a table at step 52b. The server 41 at step 51b retrieves a pass-sentence associated with the user from

its memory 44, then generates a passnumber at step 51c, before generating a table at step 51d in the manner described above in relation to Figure 1. The table is then sent at step 51e, following which the server 41 waits at step 51f for an input. When the client 42 receives the table, it displays it at step 52c, then awaits an input at step 52d. When an input is received, it is sent at step 52e to the server 41, following which the client 42 awaits a verification signal at step 52f. When an input is received at the server 41, it is compared to the passnumber at step 51g, and validity determined at step 51h. If the user is valid, a positive verification signal is sent at step 51k before the operation ends at step 51j. Otherwise, a negative verification signal is sent at step 51i, before ending at step 51j. At the client 42, the verification signal is examined at step 52g, and the user verified at step 52i or not verified at step 52j as appropriate before ending at step 52k.

An alternative system is shown in Figure 6. Referring to Figure 6, reference numerals are retained from Figure 4 for like elements. Here, the pass-sentence is stored in a memory 60 in the client 42, and the server 41 has no knowledge of it. In this embodiment, the method of Figure 1 is carried out entirely on the client 42, which the server 41 must accept as trustable. Once a user has been verified by the client 42, the user is given access to communicate with the server 41 via the client. Here, the client 42 may have knowledge of the pass-sentence because the user initially set up their account on that client, or because the pass-sentence is encrypted on a smart card read by the client, for example.

In the above embodiments, the table may, instead of being generated at random for each login, be generated by the simple reading of a table from memory. In this case, the table is the same for each login, which has the advantage that the passnumber is always the same. If the table is generated at random on each login, though, this has the advantage that the passnumber is different every time, which avoids security being compromised if a user is watched entering their input number string. Preferably, each time a table is generated at random, the same words are used, albeit in different locations. This feature prevents the pass-sentence being derivable from examination of

plural tables, with a view to seeing what word blocks are common to the tables.

In an alternative embodiment, plural tables are stored in memory, and a table is selected, preferably at random, on user login.

5 From reading the present disclosure, other variations and modifications will be apparent to persons skilled in the art. Such variations and modifications may involve equivalent and other features which are already known in the art and which may be used instead of or in addition to features already described herein. Although Claims have been formulated in this Application to particular
10 combinations of features, it should be understood that the scope of the disclosure of the present invention also includes any novel features or any novel combination of features disclosed herein either explicitly or implicitly or any generalisation thereof, whether or not it relates to the same invention as presently claimed in any Claim and whether or not it mitigates any or all of the
15 same technical problems as does the present invention. The Applicants hereby give notice that new Claims may be formulated to such features and/or combinations of such features during the prosecution of the present Application or of any further Application derived therefrom

CLAIMS

1. A method of validating a user, the method comprising:
associating a pass-sentence comprising a string of word blocks
5 (Z₁, Z₂.. Z_N) with the user;
associating a passnumber comprising a string of numeric
characters (Y₁, Y₂.. Y_N) with the user;
generating from the passnumber and the pass-sentence a table
having columns in a vertical or horizontal direction and rows in the other
10 direction, in which each word block of the pass-sentence (Z_p) is located in a
column dependent on the number of preceding word blocks (Z_{p-1}) in the pass-
sentence and in a row dependent on the corresponding character (Y_p) in the
pass-sentence;
displaying the table;
15 receiving an input comprising a string of numeric characters;
comparing the input to the passnumber; and
determining if the input is a valid input on the basis of the
comparison.
- 20 2. A method as claimed in claim 1, in which the generating step
comprises recalling the table from a storage device.
3. A method as claimed in claim 1, in which the generating step
comprises generating the table at random.
- 25 4. A method as claimed in claim 3, in which word blocks for use in
generating the table are stored in a storage device.
5. A method as claimed in claim 4, in which the number of word
30 blocks stored in the storage device is approximately equal to the number of
word block spaces in the table.

6. A method as claimed in any preceding claim, in which the table is filled with words such that each of the possible routes from a first word-filled column to a last word-filled column produces a grammatically correct sentence.

5

7. A method as claimed in claim 6, in which cells in each column are filled with words or with word strings of the same type.

8. A software product comprising computer executable instructions
10 for carrying out the method of any preceding claim.

9. Computer readable media having stored thereon a software
produce as claimed in claim 6.

15 10. A device arranged for implementing the method of any of claims
1 to 7.

11. A system arranged for implementing the method of any of claims
1 to 7.

20

12. A method of validating a user substantially as shown in and/or as
described with reference to Figure 1 or Figure 5 of the accompanying
drawings.

25

13. A device for validating a user substantially as shown in and as
described with reference to Figure 2, Figure 3 or Figure 6 of the accompanying
drawings.

30

14. A system for validating a user substantially as described with
reference to and/or as shown in Figure 4 or Figure 6 of the accompanying
drawings.

ABSTRACT

VALIDATING A USER

5 In a method of verifying a user, a pass-sentence ($Z_1, Z_2... Z_N$),
comprising a string of word blocks which in sequence form a sentence known
to the user, is associated with the user at step 12. At step 13, a pass number
($Y_1, Y_2... Y_N$) comprising a string of numbers between 0 and 9 is associated
with the user. At step 14, a table having $N+1$ columns and ten rows is
10 generated. The first column is filled with digits 0 to 9 sequentially from top to
bottom. The word blocks Z_1 to Z_8 are each included in the table thus: Z_p is
placed in column $P+1$ and in row Y_p . The other cells in the table are then filled
with suitable word blocks so that each column contains word blocks of the
same type. A user knowing their pass-sentence and seeing the table then
15 determines their passnumber by identifying the row number for which the first
word block in their pass-sentence is found, and so on, and enters it at step 16.
The input is compared at step 17 to the passnumber from step 13. If the
numbers are the same, then step 18 determines that the user is valid.

20 (Fig 1)

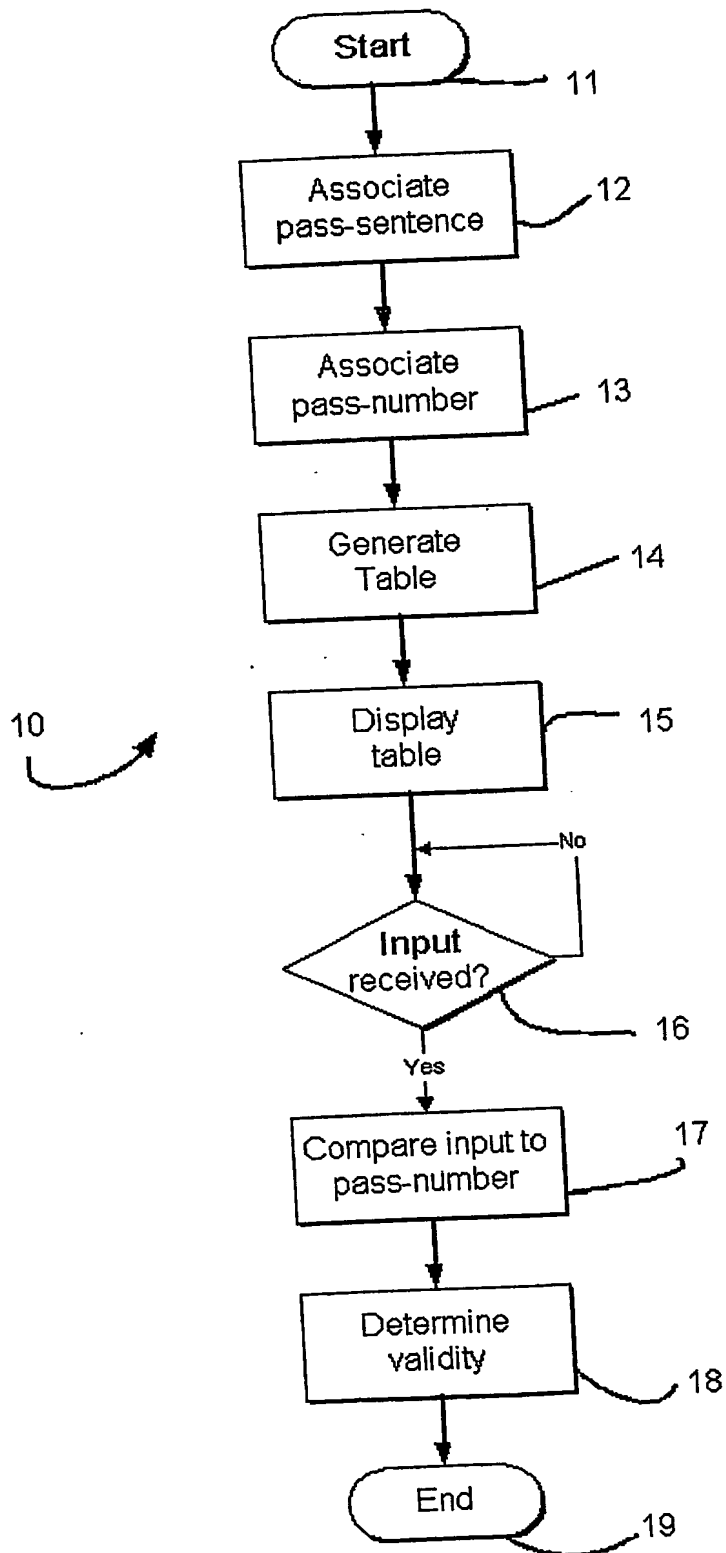


Figure 1

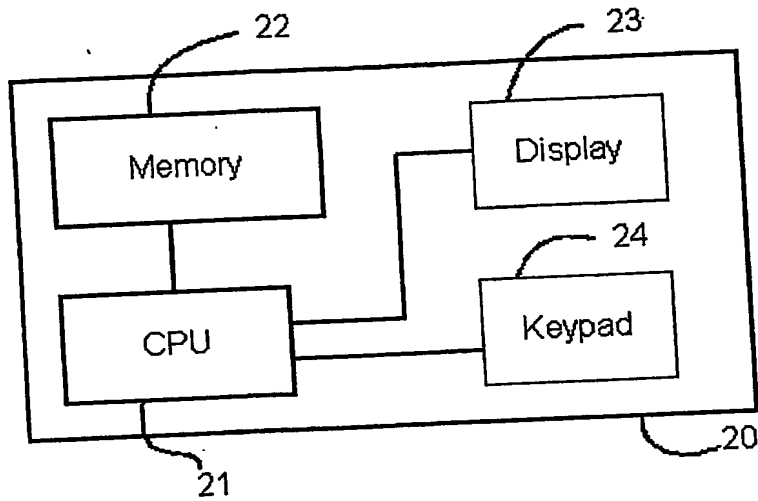


Figure 2

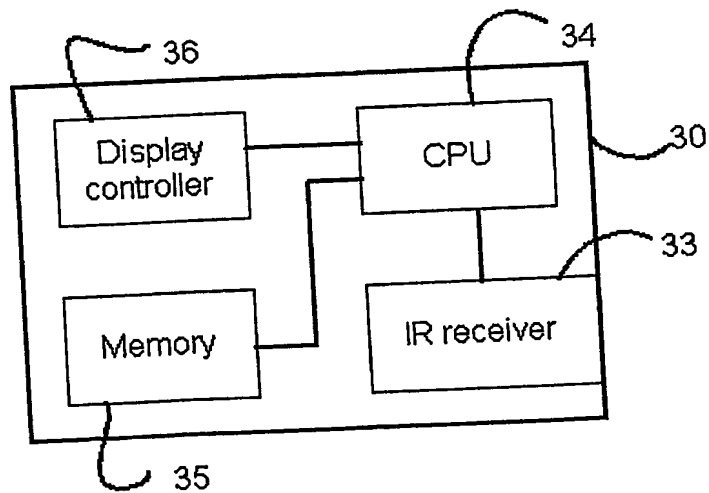
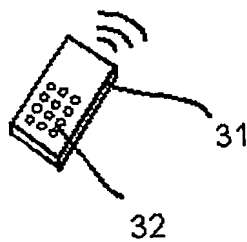


Figure 3



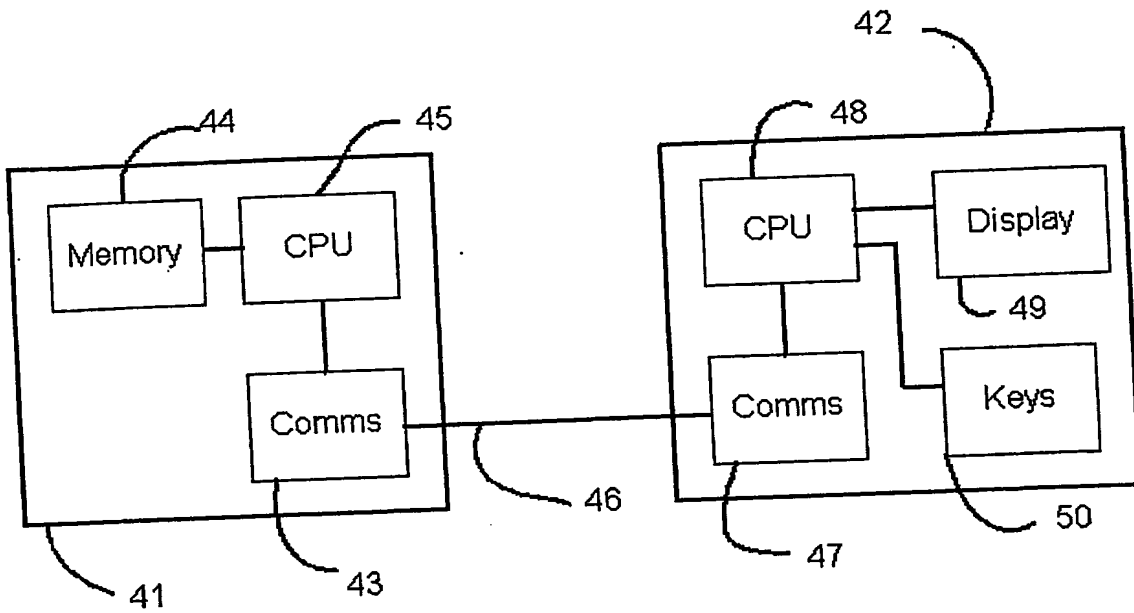


Figure 4

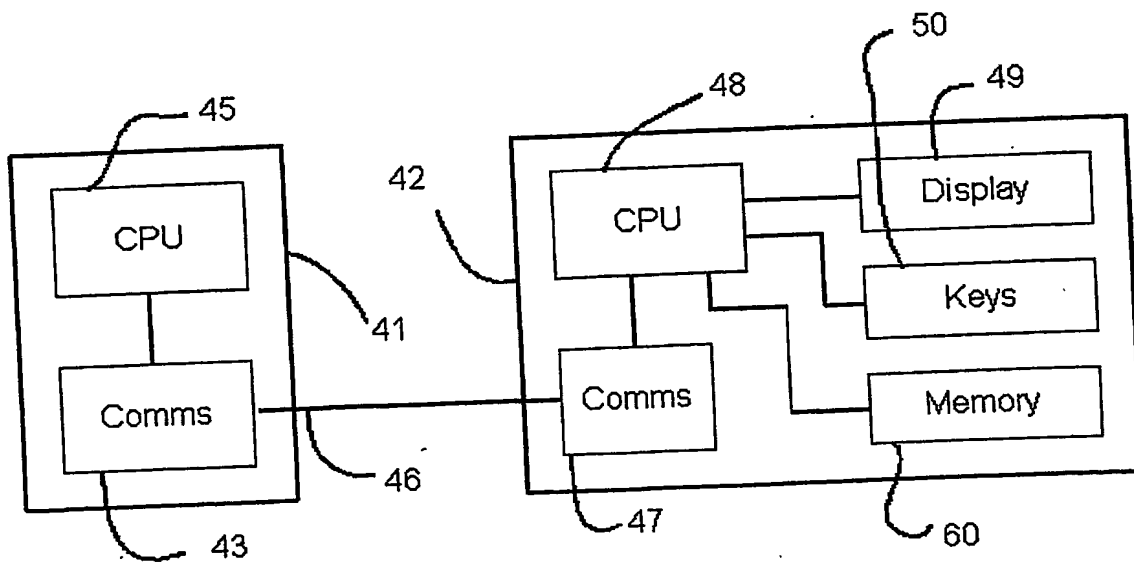


Figure 6

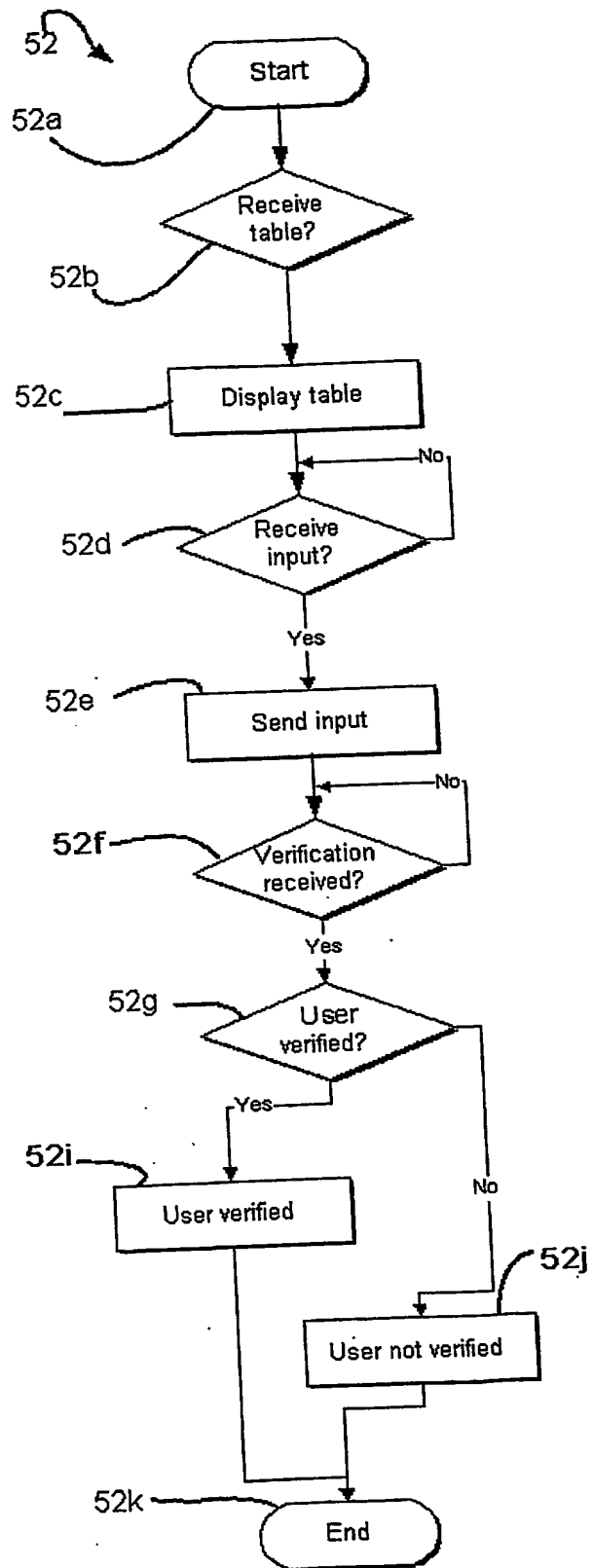
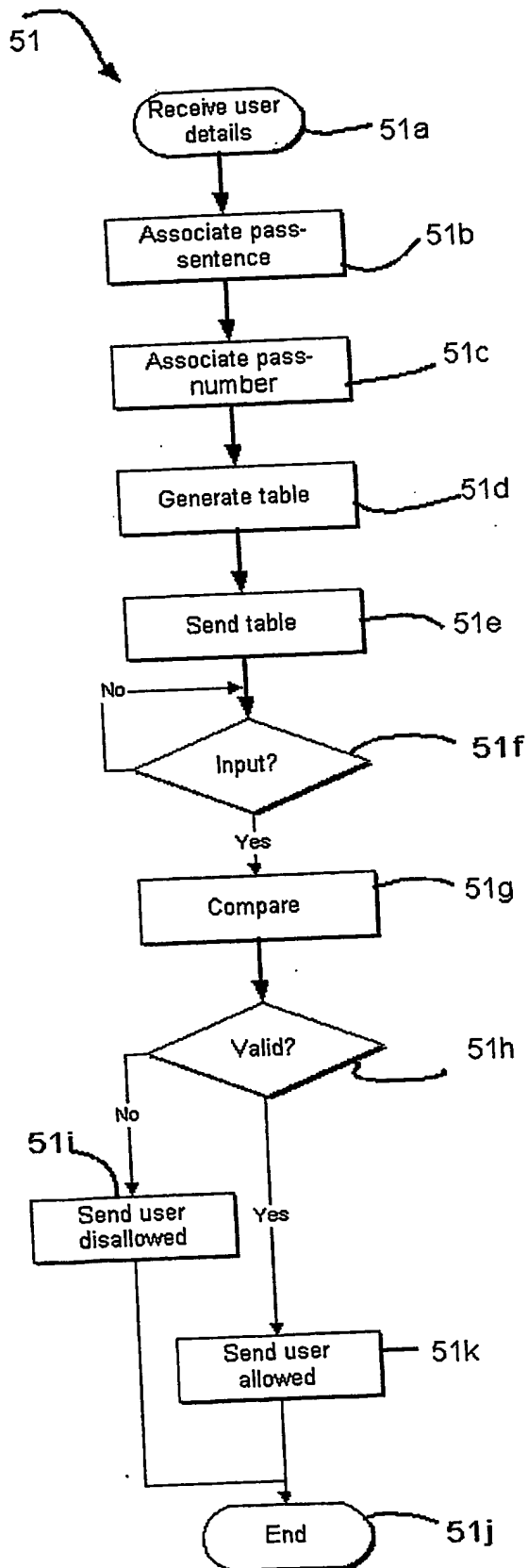


Figure 5

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.